50

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,123	06/30/2000	Martin J. Pagel	1817P	1033

7590 08/02/2005

Sawyer Law Group LLP
PO Box 51418
Palo Alto, CA 94303

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 08/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/608,123	PAGEL, MARTIN J.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 May 2005* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *28-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/19/2005 has been entered.

Response to Arguments

2. In response to communications filed on 5/19/2005, for a request to continue examination, applicant cancels claims 1-27 and amends claim 28. The following claims 28-31 are presented for examination.

2.1 Applicant's remarks, pages 4-11, filed on 5/19/2005, with respect to the rejection of claims 1-31 have been fully considered but they are not persuasive. Applicant argues that Baker does not teach verification keys generated as a function of secret key and postal destination; the verification keys are not used to create digital signature, and further argues that Baker does not teach receiving a master key and a secret key Ki. Examiner respectfully disagrees. As discussed below, the token keys are generated as a function of specific master keys and suggested using postal information in evidencing indicia as part of the authentication process (see column 1, lines 30-50 and column 2, lines 1-22) and they are used to create digital signature (column 2, lines 1-

28). Baker further discloses receiving at least two domain keys assigned to specific group of meters (see column 6, lines 50-67, column 7, lines 15-32 column 10, lines 10-20; and column 9, lines 20-52). The arguments filed on 5/19/2005 with regard to Cordery reference used in the final action are moot in view of another reference by Cordery to further support the elements disclosed in Baker, since Cordery provides more discussion on the generated keys. Upon further consideration, a new ground of rejection is made in view of Baker et al. in combination with Cordery.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1 **Claims 28-31** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,812,666 to **Baker et al.** in view of US Patent 6,058,193 to **Cordery et al.**.

3.2 **As per claim 28, Baker et al** substantially teaches method for dispensing and evidencing indicia by an indicia generating device in a system having a plurality of indicia generating devices that have been divided into n groups, each group corresponding a respective geographic designation each of the indicia generating devices for generating and printing indicia on a media that is to be received at a plurality of establishments, wherein the establishments are associated with different geographic designations, the method performed by the indicia generating devices comprising: (a) receiving master keys (postal and vendor master keys) and these keys are stored in the meter (see column 6, lines 50-56 and column 9, lines 33-36) that meets the recitation of receiving a master secret key K and a secret key Ki and storing the master secret key K and the secret key in the PGD; **Baker et al.** also discloses in response to receiving a request to generate an indicium for a medium destined for a particular one of the establishments, evidencing the indicium (column 16, line 60 through column 17, line 4 and column 17, lines 35-45). **Baker et al.** also discloses computing verification keys as a function of the received master keys (see column 5, lines 38-42 and column 17, lines 28-44), the master keys are also group specific (see column 3, lines 24-32) further discloses that computed verification keys are associated with postal destination to make authentication easier (see column 1, lines 38-50 and column 17, line 64 trough column 18, line 35) that meets the recitation of computing a verification key Vi as a function of the secret key and the postal destination and computing a key ID as a function of the master secret key and the postal destination. **Baker et al.** also discloses the use of digital signature and the message is sent including the key and the digital signature to determine whether the information contained in the message is correct; in another embodiment a meter produces a digital signature of a key record for integrity and authentication (see column 7, lines

33-58 and column 10, lines 11-21) and also discloses a digital meter signing the key registration record using the vendor and postal master keys so that the vendor and postal domains can trust that the key registration record originated at the digital meter. **Baker et al** even discloses signing the indicia with the digital tokens to provide evidence of payment to the postal and the vendor. To render the claims more obvious in combination to the suggestion provided by **Baker et al**, **Cordery et al.** in an analogous art teaches generating the digital tokens in more details by disclosing that the tokens can be generated by the meter using the received master keys and postal data (column 5, lines 1-17) that includes postal destination (column 2, lines 17-41) so information can be verified by the correct party (column 5, lines 17-30) and further discloses the meter generating signature using digital token computed from keys received by the meter for verification of indicia and meter specific information (column 2, lines 17-41 and column 3, lines 10-32). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Baker et al.** to use the generated verification key to create a digital signature for the indicia, and digitally signing the indicia by including the digital signature and the other generated token on the indicia because it would allow other party to determine whether both keys can be trusted that they actually originate from the meter. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided in **Baker et al** and **Cordery et al** to use digital signature so that the key generated for verification of indicia information can be authenticated to ensure that they originate from a trusted meter (see **Cordery et al,** column 2, lines 17-41 and column 3, lines 1-32).

As per claims 29 and 31, Baker et al. substantially teaches digital signature using any cryptographic method and combining information about the meter and the mailpiece in the verification process (column 2, lines 1-30). **Cordery et al.** in an analogous art teaches using MAC which is similar to hashing as one of the options of generating digital signature that includes key and postal data as discussed above but other method is suitable as disclosed in Cordery (column 7, line 50 through column 8 and column 2, lines 17-41). Computing keys as a one-way function is very well known in the art, for example Schneier in "Applied Cryptography" teaches that with one-way hash function, multiple signatures are easier since the same document can be signed by multiple parties without affecting the size and speed increases signature can be kept separate from the document storage requirement is much smaller. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Baker et al** to use a one-way function to benefit from the advantages known in the art as suggested by Schneier above. Therefore, these claims are rejected on the same rationale as the rejection of claim 28 above.

As per claim 30, Baker et al. discloses the limitation of using ZIP codes to designate the postal destination (see column 1, lines 30-50).

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses a multiple device key exchange using asymmetric encryption.

US Patents: 6,636,968 Rosner et al. 6,567,794 Cordery et al ; 5,878,136 Kim et al ; 5,390,251 Pastor et al.

4.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin
Patent Examiner
July 20, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100